UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/554,518	05/11/2000	LYNN D SPRAGGS	PA1317US	2076

10361	7590	12/02/2004

ANTONY C. EDWARDS
SUITE 800 - 1708 DOLPHIN AVENUE
KELOWNA, BC V1Y 9S4
CANADA

EXAMINER
HA, LEYNNA A

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

		Application No.	Applicant(s)
Office Action Summary		09/554,518	SPRAGGS, LYNN D
		Examiner	Art Unit
		LEYNNA T. HA	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>27 May 2004</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 7-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, and 7-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All   b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>5/11/2000</u>.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____ .

DETAILED ACTION

1.   **Claims 1-3 and 7-42 have been examined and Applicant has canceled claims 4-6.**

2.   **Claims 1-3 and 7-42 are rejected under 35 U.S.C. 112, 1st paragraph.**

3.   **Claims 1-3 and 7-42 are rejected under 35 U.S.C. 102(e).**

4.   **Minor informalities.**

5.   **Examiner's response.**

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6.   **Claims 1-3 and 7-42 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.**

The following claims disclose new subject matter was not mentioned nor explained in the specification or in the originally filed claims.

Claims 1 and 13: "so as to form a decrypted data file and so as to use the decrypted data file to form at least part of" the encryption key

Claims 1,7, 13, 17, 24, 27, 28, 31, 34, and 42: " without transmitting to the server either the password, the encrypted data file or the decrypted data file"

Claim 42: "means at the remote computer and isolated from the server computer for receiving the authenticated password" and

"means for generating an encryption key at the remote computer using the decrypted first data file, for encrypting a second data file at the remote computer to form an encrypted second data file for transmission to the server using the encryption key"

All dependent claims are also rejected due to their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or

indirectly from an international application filed before November 29, 2000. Therefore,

the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the

amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7.   Claims 1-3 and 7-42 are rejected under 35 U.S.C. 102(e) as being

anticipated by Thomlinson, Et Al. (US 6,532,542).

As per claim 1:

Thomlinson teaches a system for authenticating an encryption key of a

user at a remote computer remotely networked to a server computer,

comprising:

a decrypt engine in the remote computer for using a password (col.10,

lines 1-6) provided by the user to decrypt in the remote computer an encrypted

data file (col.10, lines 12-15) provided by the user into the encryption key of the

user (col.10, lines 15-25).

As per claim 2:

Thomlinson teaches the encrypted data file is stored on an RF smart card

(col.7, lines 2-10).

As per claim 3:

Thomlinson teaches the encrypted data file includes encrypted biometric data

identifying the user (col.9, line 54).

As per claim 7:

Thomlinson teaches a method for providing an authenticated encryption key of a user at a remote computer remotely networked to a server computer, comprising the steps of providing an encrypted data file to the remote computer (col.10, lines 43-45), providing a password (col.10, lines 1-3), and decrypting the encrypted data file using the password into an authenticated encryption key of user (col.11, lines 2-25).

As per claim 8:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 9:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 10:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). Hence, a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 11:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein the method includes a scanner as one of the input devices used to enter commands and information to the computer (col.5, lines 24-28) and biometric authentication

procedures (col.9, lines 47-54). Thus, it is inherent that Thomlinson teaches the method of generating biometric data of the user by scanning the biometric feature of the user and comparing the generated biometric data of the user to the data derived from the encrypted data file to authenticate the encryption key of the user (col.10, lines 30-42).

As per claim 12:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). A digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 13:

Thomlinson discloses a computer accessible medium comprising program instructions (col.4, lines 35-36) for providing an authenticated encryption key of a user by using a password provided by the user to decrypt in a remote computer an encrypted data file provided by the user into an authenticated encryption key of the user (col.10, lines 1-46).

As per claim 14:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). A digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 15: See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 16:

As rejected with the same rationale of claim 14 and further includes Thomlinson discussing the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). A digitized fingerprint of the user is inherently one of many types of biometric data by scanning the biometric feature of the user (col.5, lines 24-28).

As per claim 17:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input device used to enter commands and information such as a keyboard to receive a password from a user (col.5, lines 24-28). Further, Thomlinson include memory for storing an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer an authenticated encryption key of the user (col.10, lines 15-25).

As per claim 18:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 19:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 20:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54) and that a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 21:   See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 22:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein the method includes a scanner as one of the input devices used to enter commands and information to the computer (col.5, lines 24-28) and biometric authentication procedures (col.9, lines 47-54).   It is inherent that Thomlinson teaches the method of generating biometric data of the user by scanning the biometric feature of the user such as the fingerprint of the user. See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 23:   See col.11, lines 7-12; discussing the server configured to receive data encrypted using the authenticated encryption key.

As per claim 24:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input device used to enter commands and information such as passwords from the user (col.5, lines 24-28). Further, Thomlinson include an RF smart card (col.7, lines 2-10) for storing an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer an authenticated encryption key of the user (col.10, lines 15-25).

As per claim 25:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 26:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). A digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 27:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input devices used to enter commands and information such as a keyboard for

entering passwords from the user and a scanner (col.5, lines 24-28) for biometric authentication procedures (col.9, lines 47-54). Further, Thomlinson include an RF smart card (col.7, lines 2-10) for storing an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer an authenticated encryption key of the user (col.10, lines 15-25). Thomlinson discuss a biometric reader for generating biometric data of the user (col.7, lines 6-10).

As per claim 28:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein includes an input device used to enter commands and information such as a keyboard to receive a password from a user (col.5, lines 24-28). Further, Thomlinson include memory for storing an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer an authenticated encryption key of the user (col.10, lines 15-25).

As per claim 29:

Thomlinson teaches the encrypted data file includes encrypted biometric data

identifying the user (col.9, line 54).

As per claim 30:

Thomlinson teaches the encrypted data file is stored on an RF smart card

(col.7, lines 2-10).

As per claim 31:

Thomlinson discusses the different types of access styles that can be used to

access items (data files) in protected storage wherein includes an input devices

used to enter commands and information such as a keyboard for entering

passwords from the user and a scanner (col.5, lines 24-28) for biometric

authentication procedures (col.9, lines 47-54). Thomlinson discuss a biometric

reader for generating biometric data of the user (col.7, lines 6-10). Further,

Thomlinson include memory for storing an encrypted data file including an

encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a

password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-

15) so as to form a decrypted data file and so as to use the decrypted data file

to generate in the remote computer an authenticated encryption key of the user

(col.10, lines 15-25). In addition, Thomlinson discloses a master key used to

decrypt an appropriate item key and corresponding item authentication key.

See col.10, lines 2-21; discussing the password or other logon procedure where

Thomlinson inherently includes password and biometric verification as the

logon procedure (col.9, lines 52-54) and discusses comparing or verifying the encrypted data file (col.12, lines 2-59).

As per claim 32: See col.10, lines 2-6 and lines 40-42; discussing the password or other logon procedure where Thomlinson inherently includes password and biometric verification as the logon procedure (col.9, lines 52-54). See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 33:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54). A digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 34:

Thomlinson includes memory for storing an encrypted encryption key (col.10, lines 35-36) and includes an input devices used to enter commands and information such as a keyboard for entering a password from the user (col.5, lines 24-28) that is required the use of the password to decrypt the encrypted encryption key to form a decrypted encrypting key (col.10, lines 18-23).

As per claim 35:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 36:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54).

As per claim 37:

Thomlinson teaches the encrypted data file includes encrypted biometric data identifying the user (col.9, line 54) and a digitized fingerprint of the user is inherently one of many types of biometric data.

As per claim 38:   See col.10, lines 2-6 and lines 40-42; discussing the password or other logon procedure where Thomlinson inherently includes password and biometric verification as the logon procedure (col.9, lines 52-54). See col.12, lines 2-59; discussing the comparing or verifying process of the encrypted data file.

As per claim 39:

Thomlinson discusses the different types of access styles that can be used to access items (data files) in protected storage wherein the method includes a scanner as one of the input devices used to enter commands and information (col.5, lines 24-28) for biometric authentication procedures to the computer (col.9, lines 47-54). Thus, it is inherent that Thomlinson teaches the method of generating biometric data of the user by scanning the biometric feature of the user such as the fingerprint of the user.   See col.10, lines 2-6 and lines 40-42; discussing the password or other logon procedure where Thomlinson inherently includes password and biometric verification as the

logon procedure (col.9, lines 52-54) and comparing or verifying process by decrypting the encrypted encryption key (col.11, lines 15-18).

As per claim 40:

Thomlinson teaches the encrypted data file is stored on an RF smart card (col.7, lines 2-10).

As per claim 41: See col.10, lines 20-45; discussing using the decrypted encryption key to encrypt the data.

As per claim 42:

Thomlinson teaches a system for authenticating an encryption key of a user at a remote computer remotely networked to a server computer and transmitting secure data to the server computer, the system comprising an encrypted data file including an encryption key of the user (col.11, lines 7-26) and a decrypt engine for using a password (col.10, lines 1-6) to decrypt an encrypted data file (col.10, lines 12-15) so as to form a decrypted data file and so as to use the decrypted data file to generate in the remote computer an authenticated encryption key of the user (col.10, lines 15-25). In addition, Thomlinson discloses a master key used to decrypt an appropriate item key and corresponding item authentication key.

Claim Objections

8.   Claim 42 is objected to because of the following informalities: on

line 14 states "second date file" is misspelled and should be corrected to

"second data file". **Appropriate correction is required.**

Response to Arguments

**9.   Applicant's arguments with respect to claims 1-3 and 7-42 have

been considered but are moot in view of the new ground(s) of rejection.**

The Examiner has reviewed the amended claims and the newly added

claim 42. According to the specification and the originally filed claims, claims

1,7, 13, 17, 24, 27, 28, 31, 34, and 42 discloses new subject matter. The new

matter was neither discussed nor explained to the scope of the subject matter.

Therefore, claims 1-3 and 7-41 with the originally claimed subject matter

remains rejected with the same prior art and the new matter will not be

subjected to a rejection because it was not originally filed. The newly added

claim 42 would only be rejected to subject matter that was previously

discussed or within the specification. Any new matter will not be reviewed for

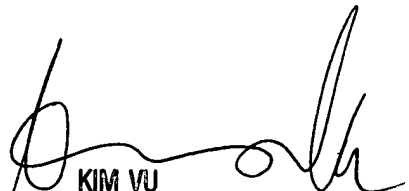examination or as part of the claim rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is **(571) 272-3851**. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306 and telephone number for TC 2100 receptionist is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

KIM VU
SUPERVISORY PATENT EXA
TECHNOLOGY CENTER